DUAL Cyber

Rischi invisibili, difese tangibili: Il Commercialista nell'era della Cybersecurity

Erika Chemello, Head of Cyber Southern Europe
Brescia, 3 Dicembre 2025

I sinistri Cyber: casi concreti

I sinistri cyber: casi concreti

01. Attacco ai server di uno studio di commercialisti con conseguente richiesta di riscatto

02. Cosa è successo?

Obiettivo dell'attacco: criptazione dei file ed esfiltrazione dei dati, con richiesta di riscatto

Il Gruppo hacker (LV Blog) ha rivendicato l'attacco rendendolo pubblico

Lo studio dichiarato di aver respinto l'attacco e che l'esfiltrazione dei dati è stata minima e non relativa ad i clienti

Risonanza mediatica che ha coinvolto anche i telegiornali

03. Svolgimento e costi sostenuti

1. Identificazione dell'attacco – incaricata società di esperti forensi
2. Identificazione delle modalità di intrusione – incaricata società di esperti forensi
3. Identificazione dei dati esfiltrati (dati personali, dati aziendali, dati sensibili ect)
4. Valutazione delle conseguenze di una pubblicazione di tali dati
5. Bonifica del server infetto – incaricata società di esperti forensi
6. Ripristino dei backup (qualora presenti) – incaricata società di esperti forensi
7. Notifica al garante relativamente all'esfiltrazione di tali dati - incaricata società legale e di consulenza
8. Notifica ai i diretti interessati dell'esfiltrazione di tali dati - incaricata società legale e di consulenza
9. Gestione delle pubbliche comunicazioni

I sinistri Cyber: casi concreti

01

Sfruttamento vulnerabilità software non aggiornato con esfiltrazione di dati

Studio di Commercialisti vittima di un'intrusione nei sistemi IT con conseguente esfiltrazione di dati dei clienti (es. contabilità, bilanci, dichiarazioni). I dati vengono parzialmente cancellati e rivenduti nel dark web.

La finalità dell'attacco è quella di esfiltrare dati ad alto valore economico rivendibili o riutilizzabili per future truffe (es. frodi fiscali, furti di identità). Non vi è una richiesta di riscatto, normalmente l'attacco è silenzioso e mirato alla monetizzazione dei dati rubati.

Dopo mesi, viene scoperta l'esfiltrazione sistematica di circa 2GB di dati. Lo studio è obbligato a notificare l'accaduto al Garante e ad informare i diretti interessati.

02

Garanzie attivabili

VIOLAZIONE DEI DATI per eventuali richieste di risarcimento in seguito al furto e alla divulgazione dei dati personali e/o aziendali

RIPRISTINO DATI E SISTEMA INFORMATICO per il recupero e/o la sostituzione di dati elettronici e/o di software persi o danneggiati

SPESE DERIVANTI DA VIOLAZIONI DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E AZIENDALI per l'attività di esperti incaricati per identificare l'origine dell'evento e per notificare gli organi di controllo

DANNI REPUTAZIONALI (se attivata) per l'attività di esperti a tutela dell'immagine dello studio

I sinistri Cyber: casi concreti

01

Attacco di tipo Ransomware attacco con richiesta di riscatto;

Criptati i dati dell'azienda; nello specifico si tratta di un grosso studio professionale.

L’attacco ha determinato il blocco dell'attività per 9 giorni

L’hacker potrebbe essere entrato in possesso di dati dei clienti dello studio, si è reso quindi necessario inviare una segnalazione all'Autorità garante per la violazione della privacy.

02

Come ha operato la polizza

Risultate attivabili le seguenti garanzie:

DANNI DA INTERRUZIONE DELL’ATTIVITÀ

Indennizzato danno per circa € 70.000 (interruzione di 9 giorni)

RIPRISTINO DATI

Indennizzati i costi sostenuti per identificare l'attacco e mitigarne le conseguenze per circa € 100.000

Risultato

Indennizzo complessivo superiore a € 170.000

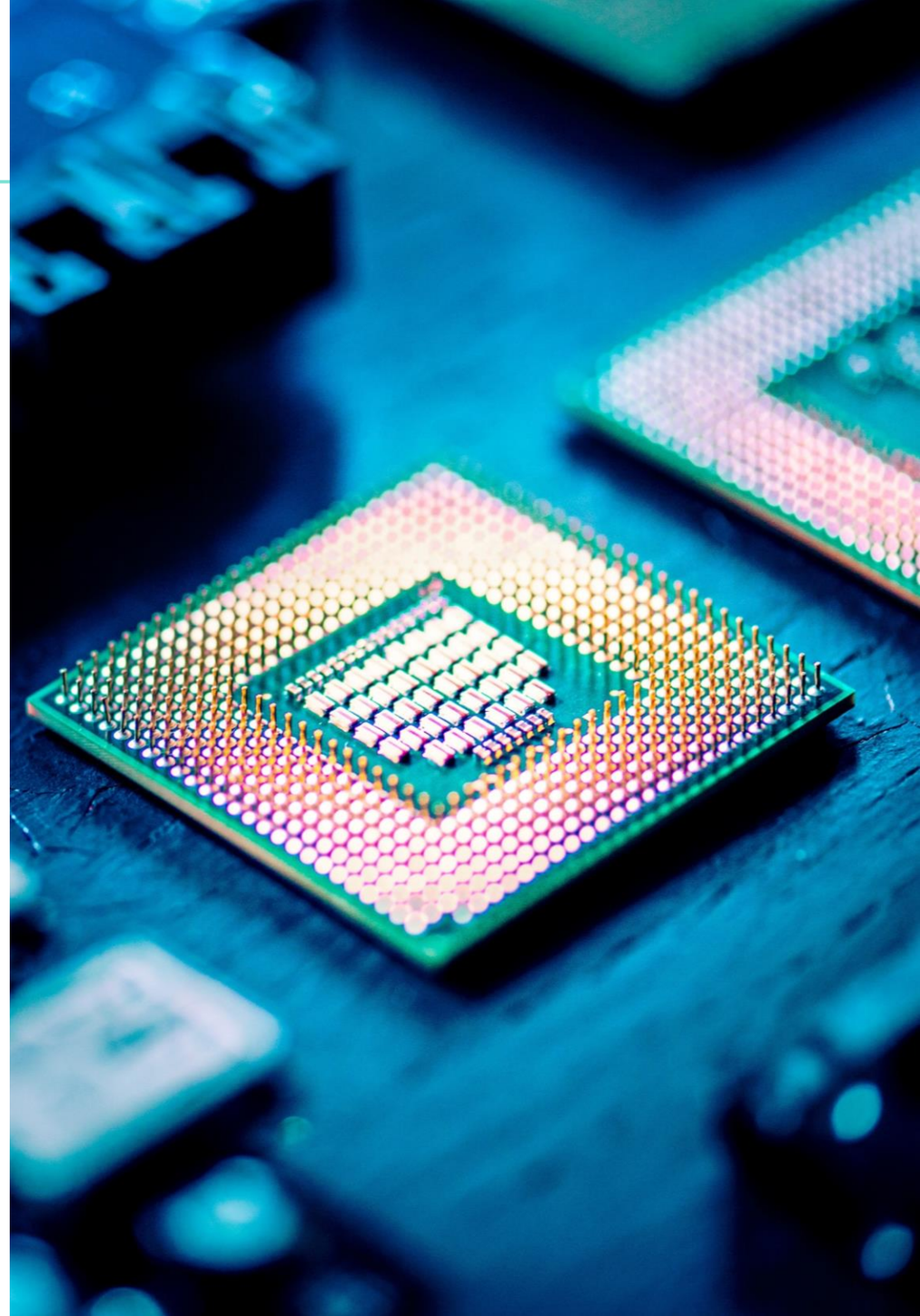
Fattori di vulnerabilità nei sistemi

Fattori tecnologici

L'arretratezza dell'architettura IT o il mancato aggiornamento dei sistemi che possono così essere presi di mira da hacker per perseguire i propri scopi malevoli

Fattori umani

Si stima che una percentuale cospicua degli attacchi informatici siano deteminati dal comportamento umano: la scarsa consapevolezza dei singoli rispetto alle policy aziendali e alle buone pratiche di comportamento introdotte in azienda determinano un aumento della vulnerabilità dei sistemi



La gestione del rischio

La gestione del rischio

Cosa non può mancare

Consapevolezza

Piani di risposta agli incidenti

Procedure Formali

Tempestività

La gestione del rischio

Strumenti

Strumenti di cybersecurity:

- **Protezione Antivirus** costantemente aggiornata su tutti i dispositivi
- **Backup offline** di tutti i dati almeno bisettimanale
- **Firewall** gestiti e configurati adeguatamente
- **Formazione**

La gestione del rischio

Strumenti

Strumenti di trasferimento del rischio:

Polizze contro gli attacchi informatici

Garanzie di responsabilità civile verso terzi

- divulgazione non autorizzata di dati
- trasmissione di virus

Garanzie indennitarie che coprono i costi vivi per gestire l'evento

- esperti informatici e legali
- esperti nella gestione delle estorsioni

Garanzie per indennizzare l'impatto economico negativo a fronte di un blocco dell'attività

Garanzie a copertura dei trasferimenti fraudolenti di fondi

Pronto intervento 24/7 in lingua italiana in caso di sinistro!

Contatti

Per maggiori informazioni, per una consulenza o una valutazione contatta:

Marco Ferrari

marco.ferrari@sigmabrescia.it

+39 338 3096548

Davide Ferrari

davide.ferrari@sigmabrescia.it

+39 349 6666405

SIGMA STUDI Brescia
Broker di Assicurazioni